



MATTHEW L. SCHWARTZ
Tel.: (212) 303-3646
E-mail: mlschwartz@bsfllp.com

January 12, 2018

BY ECF

Honorable Katharine H. Parker
United States Magistrate Judge
Southern District of New York
500 Pearl Street, Suite 1950
New York, New York 10007

**Re: *City of Almaty, Kazakhstan, et ano. v. Mukhtar Ablyazov, et al.*,
Case No. 15 Civ. 5345 (AJN) (KHP)**

Dear Judge Parker:

We represent the City of Almaty, Kazakhstan and BTA Bank (“the Kazakh Entities”). The Kazakh entities have requested that Defendants Ilyas and Viktor Khrapunov produce archives of documents that include communications stolen from Kazakh government officials by computer hackers. These archives were once publicly available but are no longer. And the Khrapunovs claim to have already produced portions of these archives in this action. They have nevertheless refused to produce the entire archives, claiming (incorrectly) that they are protected by the attorney work product doctrine. We write to respectfully request an order compelling the Khrapunovs to produce the archives in their entirety because (1) the attorney work product doctrine does not protect stolen documents; (2) even if it applied, the attorney work product doctrine was waived when the Khrapunovs decided to produce portions of the archives; and (3) even if it applied and had not been waived, under Federal Rule of Civil Procedure 26(b)(3)(A)(ii), the Kazakh entities have a substantial need for the archives and cannot obtain them elsewhere.

Background

On June 27, 2017, the Khrapunovs moved to re-open the deposition of BTA Bank’s Rule 30(b)(6) designee, Nurlan Nurgabylov, in order to question him using communications stolen from the e-mail accounts of officials of the Republic of Kazakhstan (the “Hacked Documents”). The Kazakh Entities then cross-moved for a protective order barring the use of the Hacked Documents. [ECF No. 356]. In opposing that cross-motion, the Khrapunovs represented that the Hacked Documents had been “publicly available and they were downloaded during several visits to the Kazaword website” and that a Swiss bailiff had been engaged by Ilyas Khrapunov “to create a contemporaneous record that the documents were available on the web and of the steps taken to download the documents from the website.” [ECF No. 358, at 2].

The Khrapunovs attached affidavits from this Swiss bailiff that revealed two things. First, on February 16, 2015, Ilyas Khrapunov’s lawyer downloaded fourteen archive files from an internet-based storage platform linked by Kazaword onto a flash drive and then gave a copy of the flash drive to the bailiff. Second, on October 6, 2016, Ilyas Khrapunov, in the presence of his attorneys and the bailiff, downloaded more archive files from kazaword.wordpress.com onto a flash drive and again gave a copy of the flash drive to the bailiff. *See* Ex. A, at 3; Ex. B, at 8 (originally filed under ECF Nos. 358-02, 358-03). Collectively, we refer here to those sets of downloaded archive files as the “Kazaword Archives.”

The Kazakh Entities served a document request on the Khrapunovs seeking production of the Kazaword Archives. *See* Ex. C, at 8. The Khrapunovs refused to produce them, claiming that the Kazakh Entities' request "calls for material protected by the attorney work product doctrine. On this basis, the Khrapunovs will not produce documents responsive to this Request." *See* Ex. D, at 5.

Argument

1. The Kazaword Archives are Not Protected Work Product

The Khrapunovs' cannot hide the Kazaword Archives behind the attorney work product doctrine because the files were obtained as part on an illegal computer hacking scheme. "[N]either the attorney-client privilege nor the attorney work-product doctrine protect communications made in furtherance of a crime or fraud." *Amusement Indus., Inc. v. Stern*, 293 F.R.D. 420, 425 (S.D.N.Y. 2013) (citing *In re Grand Jury Subpoena Duces Tecum Dated Sept. 15, 1983*, 731 F.2d 1032, 1038 (2d Cir.1984). "[A] party seeking to invoke the crime-fraud exception must at least demonstrate that there is probable cause to believe that a crime or fraud has been attempted or committed and that the communications were in furtherance thereof." *In re Richard Roe, Inc.*, 68 F.3d 38, 40 (2d Cir. 1995). Here, that burden is easily met.

Nicolas Bourg, a witness Judge Nathan found credible [ECF No. 175 at 5, n.4], testified that Ilyas Khrapunov commissioned computer hackers to steal and gain unlawful intelligence from the communications of foreign government officials and then selectively disclosed that information as part of a legal and media campaign. [ECF No. 482-19]. That hacking was plainly unlawful. And the hacked documents were also — according to the Khrapunovs, at least — part of the archives that Ilyas Khrapunov downloaded in the presence of counsel.¹ Downloading stolen documents in front of lawyers, however, does not change the fact that they were illegally obtained by Khrapunov in the first place. Were it otherwise, any hacker could protect the fruits of his criminal acts by putting them on a new computer in the presence of this attorney. Accordingly, because the Kazaword Archives were created to further the use of stolen communications, they are not entitled to attorney work product protection.

2. The Khrapunovs Waived Any Work Product Protections Over the Kazaword Archives

Even assuming work product protection applies to the Kazaword Archives, which it does not, the Khrapunovs waived that protection by selectively producing documents from those archives. *See Bovis Lend Lease, LMB, Inc. v. Seasons Contracting Corp.*, No. 00-Civ.-9212 (DF), 2002 WL 31729693, at *5 (S.D.N.Y. Dec. 5, 2002) ("Where a party selectively discloses certain privileged or work product material, but withholds similar (potentially less favorable) material, principles of fairness may require a more complete disclosure."); *Gruss v. Zwirn*, No. 09-Civ.-6441 (PGG), 2013 WL 3481350, at *12 (S.D.N.Y. July 10, 2013) (when party selectively discloses protected material to an adverse party, "the privilege is waived not only as to the materials provided, but also as to the underlying source materials.").

The Khrapunovs produced the Hacked Documents and attempted to use them at Mr. Nurgabylov's deposition. When the Kazakh Entities' moved for a protective order, the Khrapunovs denied that they involved in any hacking, claiming that the Hacked Documents were a

¹ Whether or not Khrapunov's Swiss counsel was aware that creating the Kazaword Archives was intended to further this scheme is irrelevant. *See Amusement Indus.*, 293 F.R.D. at 426 ("It is sufficient to come within the exception that the client intended to use the attorney's services in furtherance of a crime or fraud even if the attorney was unaware of this purpose.").

subset of the Kazaword Archives, which they purportedly downloaded from the Kazaword website while they were available. [ECF No. 358, at 2]. So long as the Khrapunovs withhold the full Kazaword Archives, however, it is impossible to test the truth of this claim – and the truth matters here. Because if the Hacked Documents are not found in the Kazaword Archives, the Khrapunovs’ claim to have innocently obtained them from a public source will be provably false.² By selectively producing the Hacked Documents, and then putting the contents of the Kazaword Archives at issue, the Khrapunovs have made the Kazaword Archives fair game in discovery, and have no basis for withholding them. *See Bovis Lend Lease*, at *5. (“Waiver of privilege and work product protection may also result from a party’s injection of an issue into the litigation that, in fairness, requires the party to disclose otherwise protected material”); *In re Kidder Peabody Sec. Litig.*, 168 F.R.D. 459, 470 (S.D.N.Y. 1996) (a party “may waive the privilege if he makes factual assertions the truth of which can only be assessed by examination of the privileged communication”).

3. *The Kazakh Entities Have a Substantial Need for the Kazaword Archives*

Finally, the Kazaword Archives should be produced because the Kazakh Entities have a substantial need for them and cannot obtain them elsewhere. *See* Fed. R. Civ. P. 26(b)(3)(A). The Kazakh Entities’ need is plain: the Court has allowed Defendants to use of the Hacked Documents in discovery for specific purposes — and has reserved decision on the question of whether they may be used at trial or in support of summary judgment — but the Kazakh Entities have no way of knowing what other materials exist in the Kazaword Archives that refute, clarify, or provide context to the documents the Khrapunovs have selectively produced. The archives are no longer accessible, and the Court has recognized that “there is no dispute that the hacked documents are no longer readily available on the internet,” and that the Kazakh Entities are “unable to determine whether documents that purport to have been obtained from the website were in fact posted.” [ECF No. 368, at 4]. Thus, other than the Khrapunovs, there is no source for obtaining these documents. *See Nat’l Cong. for Puerto Rican Rights v. City of New York*, 194 F.R.D. 105, 110 (S.D.N.Y. 2000) (finding substantial need where documents held by one party were no longer publicly available).

The Kazaword Archives do not reflect any attorney insight or trial strategy, and thus are not afforded any additional protection under Rule 26(b)(3)(B). The affidavits filed by the Khrapunovs establish that the Kazaword Archives were created by simply downloading compressed files containing each tranche of stolen documents posted on Kazaword. [See ECF No. 358-2, at 3]. There is no plausible prejudice to the Khrapunov from having to produce the Kazaword Archives, other than they won’t be able to ambush the Kazakh Entities with selective productions in the future.

For all of these reasons, the Kazakh Entities respectfully request the Court order the Khrapunovs to produce the Kazaword Archives.

Respectfully,

/s/ Matthew L. Schwartz
Matthew L. Schwartz

² Of course, even if the Hacked Documents appear in the Kazaword Archives, that would not prove Ilyas Khrapunov was not involved in the underlying theft. Indeed, Ilyas Khrapunov appears to have tried to launder the Hacked Documents by putting them up on Kazaword — a website he controls, *see* Ex. A, at 3 (affidavit of Swiss bailiff engaged by Ilyas Khrapunov, referring to “my principle’s website, at the following address: <https://kazaword.wordpress.com>”) — and then re-downloading them in the presence of counsel.